

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

information associated with Apple ID
barasnehyousef@gmail.com that is stored
at premises controlled by Apple

Case No. 20-878M(NJ)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property over which the Court has jurisdiction pursuant to Title 18, United States Code, Sections 2703 and 2711:

See Attachment A

I find that the affidavit(s) or any recorded testimony, establish probable cause to search and seize the person or property described above and that such search will reveal:

See Attachment B

YOU ARE COMMANDED to execute this warrant ON OR BEFORE February 7, 2020 (not to exceed 14 days)
☐ in the daytime between 6:00 a.m. and 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Nancy Joseph
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued:

January 24, 2020
@ 11:35 am

Nancy Joseph
Judge's signature

Return

Case No:

20-878M

Date and time warrant executed:

1-24-20 @ 2:15pm

Copy of warrant and inventory left with:

Apple Legal via email

Inventory made in the presence of:

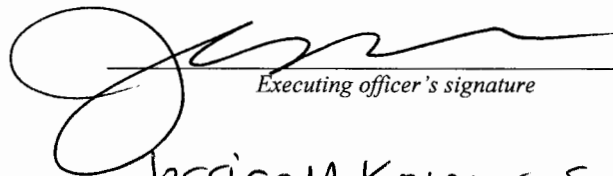
Apple provided return via email

Inventory of the property taken and/or name of any person(s) seized:

Records pertaining to Apple account
baranahyousel@gmail.com**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the undersigned judge.

Date: 2-13-20



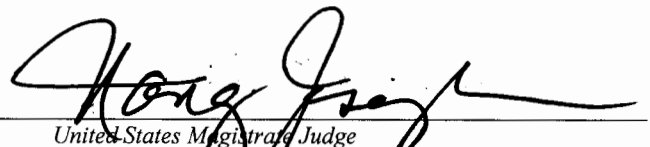
Executing officer's signature

Jessica M Kneyer, Special Agent

Printed name and title

Subscribed, sworn to, and returned before me this date:

Date: 2/13/20



United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with
barasnehyousef@gmail.com (the “account”) that is stored at premises owned,
maintained, controlled, or operated by Apple Inc., a company headquartered at
Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"),

Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from March 1, 2019 to present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from March 1, 2019 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant

message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

- h. All records pertaining to the types of service used;
- i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
- j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 10 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of 18 U.S.C. § 241 involving Yousef Omar Barasneh since March 1, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Records and information relating to a conspiracy to injure, oppress, threaten, and intimidate minority citizens, including Jewish citizens, in the free exercise of their legal rights, including the right to hold and use real and personal property in the same manner as that right is enjoyed by white citizens, as guaranteed by Title 42, United States Code, Section 1982;
- b. Records and information relating the organization known as The Base, associates of The Base, or white supremacy ideology, including any communications;
- c. Records and information relating to the Beth Israeli Sinai Congregation;
- d. Records and information relating to targets or potential targets of threats, harassment, or intimidation by the Base or otherwise based on white supremacist ideology
- e. The identity of the person(s) who created or used the Apple ID;

f. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

g. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

h. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

i. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple, as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature